Technology Bucket	Category	Description
Blockchain & Cybersecurity	Software	Provide ideas in a decentralized and distributed ledger technology used to store digital information that powers cryptocurrencies and NFTs and can radically change multiple sectors
Blockchain & Cybersecurity	Hardware	Provide ideas in a decentralized and distributed ledger technology used to store digital information that powers cryptocurrencies and NFTs and can radically change multiple sectors
Blockchain & Cybersecurity	Software	An online meeting portal is needed for AICTE to ensure the secure sharing of confidential data. The system can be developed by designing the architecture, building the backend infrastructure, integrating video conferencing capabilities, creating a user-friendly interface, and implementing robust security measures.

Blockchain & Cybersecurity	Software	AICTE needs a centralized portal for managing technical education institutions' critical infrastructure and data. The portal should manage servers, firewalls, load balancers, software licenses, user access, and other data center hardware components. However, the current infrastructure management practices face challenges such as fragmented management, manual processes, and limited visibility and control.
Blockchain & Cybersecurity	Software	The Onion Routing (TOR) is an overlay anonymous network over the internet, which not only anonymizes clients accessing the TOR network or internet but also facilitates the hosting of servers anonymously. These servers have been reported to be hosting various hidden services involved in malicious activities. The goal of this problem statement is to develop a Proof of Concept (PoC) to enumerate URLs (.onion) of active hidden servers hosted over TOR. Teams are supposed to examine the cryptographic security controls and survey existing vulnerabilities in the underlying security architecture of the TOR network to develop PoC for efficient enumeration of URLs of active hidden services hosted over TOR.

Blockchain & Cybersecurity	Software	The phishing attack is the most prevalent attack technique to compromise users worldwide. Phishing links/websites are shared through several mediums like email, SMS, etc. to target users. These domains are at times host user login page that imitates the genuine target websites. Login attempts on such pages can lead to the compromise of user credentials and may also download malicious payloads to user computers. The objective of the problem is to identify such phishing domains from the newly registered websites based on open source databases (For example WHOIS Database). Such databases provide a list of newly registered domains. The tool should be automated and harness the power of AI/ML to identify phishing domains from genuine domains. It may use the following techniques: (a) Backend code / content similarity in web pages. (b) Web page image analysis (i.e. analysis between genuine and phishing site web page images; the more the similarity better the probability score of being a lookalike phishing site). The evaluation would be based on the tool's ability about the following: (e) Probability scores of phishing domains on how close they are to the genuine domain. (f) Ability to detect new phishing domains in a reasonable time. (g) Ease of use and flexibility in output formats.
Blockchain & Cybersecurity	Software	Internet Protocol Security (IPsec) is a widely used network layer security control for protecting communications. It is a framework of open standards for ensuring secure communication over IP networks. The goal of this problem statement is to identify unknown vulnerabilities in the implementation of crypto libraries used by OpenVPN for Internet Protocol Security (IPsec), and IPV6 deployment. Teams may undertake static/ dynamic analysis of relevant code to discover any unknown software bug. Emphasis should be on finding unknown vulnerabilities in the implementation of cipher suites/ crypto libraries used by OpenVPN for encryption and authentication in IPsec tunnels. Teams may also investigate and report vulnerable configurations and associated exploitation vectors leading to compromise of data confidentiality, which has not been reported so far for IPSEC IPv6 deployment using OpenVPN.

Blockchain & Cybersecurity	Software	Ransomware is a type of malicious software designed to block access to ICT devices by encryption of data until a ransom is paid to the attacker. It is of paramount importance to increase awareness regarding such attacks and assess the readiness of the ICT infrastructure of any organization to thwart these attacks or at least recover at the earliest. The developer should design and deploy a methodology to evaluate the posture and preparedness of an organization toward stopping/mitigating threats from ransomware attacks. The developed tool shall be evaluated based on the following: (a) Depth of the tool to assess the readiness of the organization to hinder/stop /mitigate ransomware attacks. (b) Assessment of organization towards detection of early signs of ransomware. (c) Ease of use and awareness imparted by the tool. (d) Visualization and reporting of the maturity assessment of the organization.
Blockchain & Cybersecurity	Software	Early detection of a compromise of any computing device is critical for the security of critical information infrastructure. While most infections on ICT are detected using IoCs (Indicators of Compromises), the objective of this problem is to explore techniques for the detection of compromise on devices using AI / ML models when the IoC of the compromise is not known. The developer should employ innovative models for non-IoCs based detection of compromise on devices. The evaluation of the solution will be based on the following: (a) Innovation and ruggedness of the method of detection of compromise. (b) Utility of the method developed over various types of devices including system/firewall/router/network. (c) Ease of deployment and method of reporting of detected compromise. (d) Ability to minimize false alarms of compromise.
Blockchain & Cybersecurity	Software	Whatever the darkest corner of the diabolical human mind can conceive, Dark-Web can deliver with anonymity and impunity. Dark web markets and forums are filled with illicit activities such as counterfeit currency, fake documents, contraband drugs, ransomware attacks, etc. In India, Dark-web crimes have proliferated in recent times, especially in the arena of terrorism, drug trafficking, counterfeit documents, currency, and the sale of classified Government documents. Governments have also recently raised concern over digital currency and the use of Dark-Web for drug trafficking. Appropriate tools and techniques must be developed to monitor and track anti-national activities carried out behind the shield of anonymity by using the dark web and cryptocurrency technology.

Blockchain & Cybersecurity	Software	Developing a data compression system for a backbone network. Proposed Solution: you can develop a data compression system for a backbone network that efficiently compresses data, reduces network bandwidth requirements, and optimizes network performance while considering the specific requirements and constraints of the network environment.
Blockchain & Cybersecurity	Software	Developing a simulator system for counter hijack and sky marshaling operations. You can develop a simulator system that provides realistic and effective training for counter-hijack and sky-marshaling operations. Collaborating with experts in aviation security, law enforcement, and simulation technology can further enhance the development process and ensure the system meets the specific needs of the training program.
Blockchain & Cybersecurity	Software	CRPF units/offices and personnel are deployed in different locations of CRPF. There is no centralized system to analyze the logs of IT systems by the experts to assess threats and breaches. Proposed Solution: A centralized system should be developed for analyzing the systems deployed at the different locations of the country Experts per problems statement
Blockchain & Cybersecurity	Software	Cyber intrusion attempts and cyber-attacks in any critical sector are carried out with malicious intent. ln Power sector, it's either to compromise the power supply system or to render the grid operation insecure. Any such compromise may result in the maloperation of equipment, equipment damages, or even a cascading grid brownout/blackout. The much-hyped air gap myth between LR and or systems now stands shattered. The artificial air gap created by deploying firewalls between any LR and or system can be jumped by an insider or an outsider through social engineering. Cyber-attacks are staged through tactics and techniques of initial Access, Execution, persistence, privilege Escalation, Defense Evasion, Command and Control, and Exfiltration. After gaining an entry inside the system through privilege escalation, the control of the lr network and operations of or systems can be taken over even remotely by any cyber adversary. The gain of sensitive operational data through such intrusions may help the Nation/State-sponsored or non-sponsored adversaries and cyber-attackers to design more sinister and advanced cyber-attacks. How to develop a centralized information security log- collection facility or Security Operation Center (SoC) in the Power Sector, considering cEA cybersecurity (power Sector) Guidelines- 2021, to keep lT and OT networking Systems isolated and air-gapped?

Blockchain & Cybersecurity	Software	The power system networks are getting automated and software is being updated or new software is being used in the network for various purposes including SCADA, Head End System, Meter Data Management System, Billing System, etc. Most of these software are loaded in demilitarized zones; regular patch updates and penetration tests are normally avoided on the live systems. These systems become vulnerable, and hackers try to exploit such systems using various attack vectors. The challenge is to validate the presence of malicious codes if any in the software that could exploit specific attacks including the zero-day attack.
Blockchain & Cybersecurity	Hardware	We know that technology is changing fast and so are the devices used in the Power Systems network. The hardware devices used in the sector also have fast processing capacity and are intelligent. They also communicate data either periodically or on request or if some logic is met or at programmed intervals, to control centers or to local/zonal SCADA systems. The devices could be Intelligent Electronic Devices (IEDs) like Relays, BCUs, Smart Meters, Remote Terminal Units (RTU), etc. As these are electronic devices, they are prone to security threats. To make sure these devices are free from security threats, it is required to test them for malware / Trojan or similar malicious codes present in the devices/ hardware systems (like System on Chip/ Microcontrollers / Microprocessors/ DSP /FPGA-based products) which has inbuilt firmware and dedicated application programs running within available and constraint memory. The challenge is to validate such electronic types of equipment for vulnerability assessment tests and the presence of suspicious or malicious codes if any, in the devices; such codes could otherwise exploit specific attacks which may cause damage to the process/ system or harm the environment and living beings on certain conditions or may trigger on logics including the zero-day attack.

Blockchain & Cybersecurity	Software	In, in today's world, using different mobile applications for specific tasks is very common. This leads to smartphone users accumulating too many applications over a period. Seldom do users delete unused applications? Any application performing malicious tasks can very easily go unnoticed. So, there is a need to develop a mobile app tool that can use open-source intelligence and threat feeds to detect various indicators of compromise in smartphones. The tool can check network communication to various lP addresses that are suspicious, various URLs that are suspicious, inbound connections, or packets from applications that are suspicious.
Blockchain & Cybersecurity	Software	Currently, a large no of training programs are organized, and certificates are provided. There is no mechanism to validate digital certificates. so create a system in which custom digital certificates are generated. Users can store certificates in a digital locker system other organizations will validate the certificate. Use open-source software and blockchain technology. Expected Output: Blockchain Certificate generation and validation Certificate can be added in Digital Loker System Users: Government Office, Student, Industry, Institutes
Blockchain & Cybersecurity	Software	The social life of everyone has become associated with online social networks. These sites have made a drastic change in the way we pursue our social life. Making friends and keeping in contact with them and their updates has become easier. But with their rapid growth, many problems like fake profiles, and online impersonation have also grown. Fake profiles often spam legitimate users, posting inappropriate or illegal content. Several signs can help you spot a social media fake trying to scam your business. Identifying fake social media profiles and taking corrective measures. Expected Output: An Application software that detects fake social media profiles Users: Crime branches and other investigative agencies

Blockchain & Cybersecurity	Software	This aims to develop a cybersecurity-enabled smart controller specifically designed for grid-connected microgrids. The smart controller will play a crucial role in ensuring the secure and efficient operation of the microgrid, protecting it from cyber threats and unauthorized access. Key Objectives: Secure Communication: Design a communication framework that employs robust encryption protocols to safeguard the data transmitted between the smart controller and various components within the microgrid. This framework should prevent unauthorized access, tampering, and eavesdropping. Intrusion Detection and Prevention: Implement advanced intrusion detection and prevention mechanisms within the smart controller to identify and mitigate potential cyber-attacks in real time. Develop algorithms and techniques to detect anomalies, malicious activities, and vulnerabilities within the microgrid system. Access Control: Create an access control mechanism for the smart controller that regulates user access based on roles and privileges. This mechanism should prevent unauthorized configuration changes and ensure that only authorized personnel can modify or interact with the microgrid system. Cybersecurity Auditing: Develop a logging and auditing system within the smart controller to track and monitor all activities and events related to the microgrid's cybersecurity. This system should provide detailed logs, alerts, and reports to facilitate post-incident analysis and forensic investigations. Security Patch Management: Implement a mechanism within the smart controller to

Blockchain & Cybersecurity	Software	The objective of this hackathon is to develop a blockchain-based eVault system for legal records that can ensure security, transparency, and accessibility for all stakeholders. The system should be able to store, manage, and share legal records securely and efficiently, with the potential to integrate with existing legal databases and case management systems. Requirements: 1. The eVault system should be based on a blockchain platform such as Ethereum, Hyperledger, or Corda, and should use smart contracts to manage access, permissions, and transactions. 2. The system should have user-friendly interfaces for lawyers, judges, clients, and other stakeholders to interact with the eVault, with features such as uploading and retrieving documents, tracking changes, and sharing information. 3. The system should ensure the privacy and confidentiality of legal records, with appropriate access controls, encryption, and authentication mechanisms. 4. The system should allow for seamless integration with existing legal databases and case management systems, to ensure interoperability and ease of use. 5. The system should be scalable and adaptable to accommodate future changes and upgrades. Expected Outcomes: 1. A functional prototype of the blockchain-based eVault system for legal records, with a user-friendly interface and features such as document upload, retrieval, and sharing. 2. A detailed design document outlining the architecture, features, and technical specifications of the eVault system. 3. A business plan outlining the potential impact, market opportunities, and revenue models for the